UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,001	07/05/2001	Mark J. McArdle	002114.P021	5140

28875 7590 03/17/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,001	MCARDLE ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-14,16-26 and 28-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-14,16-26 and 28-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 12 December 2005.

2. Claims 1, 2, 4-14, 16-26 and 28-42 are pending in the application.

3. Claims 1, 2, 4-14, 16-26 and 28-42 have been rejected.

4. Claims 3, 15 and 27 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1, 2, 4-14, 16-26 and 28-39 have been considered but are moot in view of the new ground(s) of rejection.

Response to Amendment

6. The examiner approves of the amendment made to claim 13. The applicant has removed the extra "a" that was in the claim. The grammatical error has been corrected. The examiner withdraws the claim objection claim 13.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 4-14, 16-26 and 28-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Haatainen et al U.S. Patent No. 6,678,734 B1.

As to claim 1, Haatainen et al discloses a computerized method to prevent identification of an operating system executing on a computer connected to a network comprising:

intercepting a portion of outgoing network data characteristic of the operating system [column 7, lines 11-60]; and

conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network [column 7, lines 11-60];

wherein the masking the portion comprises:

replacing the portion of outgoing network data with data characteristic of the different operating system [column 7, lines 11-60].

As to claims 2, 14 and 26, Haatainen discloses discarding the portion of outgoing network data [column 16, lines 60-65].

As to claims 4 and 16, Haatainen discloses that the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data [column 15, lines 53-65].

As to claims 5 and 17, Haatainen discloses that the security policy further specifies replacement data for the portion of outgoing network data [column 16, lines 13-59]. Haatainen discloses the replacement data characteristic of the different operating system [column 16, lines 13-59].

As to claims 6, 18 and 39, Haatainen discloses that the security policy further defines the network as untrusted [column 13, lines 21-41].

As to claims 7, 19 and 29, Haatainen discloses receiving the security policy through the network [column 13, lines 21-41].

As to claims 8, 20 and 30, Haatainen discloses modifying the security policy based on user input [column 13, lines 21-41].

As to claims 9, 21 and 28, Haatainen discloses transmitting the portion of outgoing network data unchanged if the network is a trusted network [column 14, lines 6-23].

As to claims 10, 22, 31, 37 and 38, Haatainen discloses the method further comprising:

intercepting a portion of incoming network data, as discussed above; and

sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network [column 13, lines 21-41].

As to claims 11 and 23, the Haatainen discloses that the security policy identifies the portion of incoming network data and the false response [column 14, lines 24-31].

As to claims 12, 24 and 32, Haatainen discloses that the method is integrated into a firewall that protects the computer [column 13, lines 21-41].

As to claim 13, Haatainen et al discloses a computer-readable medium having executable instructions to cause a computer to perform a method comprising:

intercepting a portion of outgoing network data characteristic of the operating system [column 7, lines 11-60]; and

conditionally masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network [column 7, lines 11-60];

wherein masking the portion comprises:

replacing the portion of outgoing network data with data characteristic of the different operating system [column 7, lines 11-60].

As to claim 25, Haatainen et al discloses a computerized system comprising:

a processing unit [column 7, lines 11-60];

a memory coupled to the processing unit through a bus [column 7, lines 11-60];

a network interface coupled to the processing unit through the buss and further operable for coupling to a network [column 7, lines 11-60];

an operating system executed from the memory by the processing unit [column 7, lines 11-60]; and

a fingerprint masking process executed from the memory by the processing unit to intercept a portion of outgoing network data characteristic of the operating system when the network interface is coupled to the network [column 7, lines 11-60], and to conditionally mask the portion of outgoing

network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network [column 7, lines 11-60];

wherein the fingerprint masking process further causes the processing unit to mask the portion by replacing the portion of outgoing network data with data characteristic of the different operating system [column 7, lines 11-60].

As to claim 33, Haatainen et al discloses that the computerized system is a firewall and the fingerprint masking process masks an operating system on a computer coupled to the firewall [column 7, lines 11-60].

As to claim 34, Haatainen et al discloses a computer-readable medium having stored thereon an OS fingerprint policy data structure comprising:

a data unit type field containing data representative of an identifier for a type of data unit, wherein information associated with the data unit is characteristic of an operating system [column 7, lines 11-60]; and

an action field containing data representative of an action to be taken to mask the information associated with the data unit identified by the data unit type field [column 7, lines 11-60];

wherein making the information comprises:

replacing the information with information characteristic of a different operating system [column 7, lines 11-60].

As to claim 35, Haatainen et al discloses the computer-readable medium further comprising:

> a re-fingerprint field containing data representative of an identifier for a field type with the data unit type identified by the data unit type field, and further containing re-fingerprint data that identifies replacement data for the field identified by the field type [column 7, lines 11-60].

As to claim 36, Haatainen et al discloses that the re-fingerprint data is selected from the group consisting of the replacement data and a location for the replacement data [column 7, lines 11-60].

As to claim 40, Haatainen et al discloses that the security policy contains data on a plurality of different operating systems for allowing the portion of outgoing network data to impersonate any one of the plurality of different operating systems [column 7, lines 11-60].

As to claim 41, Haatainen et al discloses that each of the different operating systems included in the plurality of different operating systems is assigned a specific untrusted network for masking the portion of outgoing data according to the untrusted network [column 7, lines 11-60].

As to claim 42, Haatainen et al discloses that the false response is sent if the operating system would normally not respond to the incoming network data [column 14, lines 24-41].

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
March 13, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100